AMENDMENTS TO THE CLAIMS

1   1. (previously presented): A method providing security for a plurality of data records
2   stored on a computer readable medium within a computing system , wherein
3   said computer readable medium additionally stores a first data structure,
4   starting at a first location within said computer readable medium, locating data
5   records in said plurality thereof,
6   said method comprises an encryption subroutine executed as said computing
7   system is being shut down and a decryption subroutine executed as said computing
8   system is being initialized,
9   said encryption subroutine includes receiving a request to shut down said
10   computing system, reading said first data structure from said computer readable
11   medium, encrypting said first data structure with a public key of said computing
12   system to produce an encrypted version of said first data structure that can only
13   be decrypted with a private key of said computing system to prevent reading
14   information stored in said data records with said computer readable medium
15   removed from said computing system, deleting said first data structure from said
16   computer readable medium, and storing said encrypted version of said first data
17   structure in nonvolatile storage, starting at a second location within said nonvolatile
18   storage, and
19   said decryption subroutine includes determining that electrical power has
20   been turned on in said computing system, reading said encrypted version of said
21   first data structure from said nonvolatile storage, decrypting said encrypted version
22   of said first data structure with said private key of said computing system to form
23   said first data structure, and writing said first data structure to said computer
24   readable medium, starting at said first location.

1   2. (original): The method of claim 1, wherein said second location is on said computer
2   readable medium

1   3. (original): The method of claim 2, wherein said second location is at said first location.

1   4. (original): The method of claim 1, wherein said nonvolatile storage is a memory
2   structure, separate from said computer readable medium, within said computing
3   system.

1   5. (original): The method of claim 1, wherein
2   encryption of said first data structure occurs within a cryptographic processor
3   in said computing system using an encryption key,
4   said cryptographic processor is separate from a system processor within said
5   computing system, and
6   decryption of said encrypted version of said first data structure occurs within
7   said cryptographic processor in said computing system using a decryption key
8   generated from data stored in secure storage accessed by said cryptographic
9   processor.

1   6. (canceled)

1   7. (original): The method of claim 1, wherein said encrypted version of said first data
2   structure is equal in length to said first data structure.

1   8. (original): The method of claim 1, wherein
2   said computer readable medium additionally stores a second data structure,
3   starting at a second location within said computer readable medium, describing
4   characteristics of said first data structure, and
5   said encryption subroutine additionally includes reading said second data
6   structure to determine characteristics of said first data structure

1   9. (original): The method of claim 8, wherein

2   said first data structure is a file allocation table, and

3   said second data structure is a boot record.

1   10. (original): The method of claim 8, wherein

2   said first data structure includes an array of file records in a master file table

3   of a NTFS file, and

4   said second data structure includes metafile data in said master file table.

1   11. (original): The method of claim 1, wherein

2   said method additionally comprises a configuration subroutine providing a

3   user interface for setting and resetting a configuration bit, and

4   said encryption subroutine is executed according to a state of said

5   configuration bit.

1   12. (original): The method of claim 11, wherein

2   said encryption subroutine additionally includes setting a flag bit in non-

3   volatile storage, and

4   said decryption subroutine is executed only when said flag bit is set.

1   13. (currently amended): A method providing security for a plurality of data records

2   stored on a computer readable medium within a computing system, wherein

3   said computer readable medium additionally stores a first data structure starting

4   at a first location within said computer readable medium, locating data records in said

5   plurality thereof,

6   said method comprises an encryption subroutine executed to encrypt said

7   first data structure and a decryption subroutine subsequently executed to decrypt

8   an encrypted version of said first data structure,

9   said encryption subroutine includes reading said first data structure from said

10   computer readable medium, encrypting said first data structure within a

11   cryptographic processor in said computing system using an encryption key to

12   produce an encrypted version of said first data structure to prevent reading

13   information stored in said data records with said computer readable medium

14   removed said computer system, deleting said first data structure from said

15   computer readable medium, and storing said encrypted version of said

16   first data structure in nonvolatile storage, starting at a second location

17   within said nonvolatile storage, and

18   said decryption subroutine includes reading said encrypted version of said

19   first data structure from said nonvolatile storage, decrypting said encrypted version

20   of said first data structure within said cryptographic processor in said computing

21   system using a decryption key generated from data stored in secure storage

22   accessed by said cryptographic processor to form said first data structure, and

23   writing said data structure to said computer readable medium, starting at said first

24   location.

1   14. (original): The method of claim 13, wherein

2   said encryption subroutine is executed in response to receiving a request to

3   shut down said computing system, and

4   said decryption subroutine is executed in response to electrical power being

5   turned on within said computing system.

1   15. (original): The method of claim 14, wherein

2   said method additionally comprises a configuration subroutine providing a

3   user interface for setting and resetting a configuration bit, and

4   said encryption subroutine is executed according to a state of said

5   configuration bit.

1   16. (original): The method of claim 15, wherein

2   said encryption subroutine additionally includes setting a flag bit in non-

3   volatile storage, and

4   said decryption subroutine is executed only when said flag bit is set.

1   17. (original): The method of claim 13, wherein

2   said method additionally comprises a cryptographic selection subroutine

3   providing a graphical user interface,

4   said cryptographic selection subroutine includes displaying a choice between

5   encryption and decryption, displaying representations of computer readable medium

6   in said computing system, and receiving a cryptographic selection signal indicative

7   of whether encryption or decryption is to occur and of a chosen computer readable

8   medium,

9   said encryption subroutine is executed in response to receiving a

10   cryptographic selection signal indicating encryption is to occur, with said first data

11   structure of said chosen computer readable medium being encrypted, and

12   said decryption subroutine is executed in response to receiving a

13   cryptographic selection signal indicating decryption is to occur, and with said

14   encrypted version of said first data structure of said chosen computer readable

15   medium being decrypted.

1   18. (original): The method of claim 17, wherein said encrypted version of said first data

2   structure is stored in nonvolatile storage on said chosen computer readable

3   medium.

1   19. (previously presented): A computing system providing secure storage of a

2   plurality of data records comprising:

3   a first computer readable medium storing said plurality of data records and

4   a first data structure providing locations and sequences for accessing data within

5   said data records;

6   a first drive unit recording data on said first computer readable medium and

7   reading data from said computer readable medium;

8   nonvolatile storage;

9   a cryptographic processor, wherein said cryptographic processor is

10   programmed to execute an internal encryption routine to encrypt a data structure,

11   forming an encrypted version of said data structure using an encryption key, and to

12   execute subsequently an internal decryption routine, decrypting said encrypted

13   version of said data structure, using a decryption key;

14   secure storage. accessed by said cryptographic processor, holding data used

15   within said cryptographic processor to derive said decryption key;

16   a microprocessor, separate from said cryptographic processor, wherein said

17   microprocessor is programmed to execute a data structure encryption routine to

18   encrypt said first data structure and to execute subsequently a data structure

19   decryption routine to decrypt an encrypted version of said first data structure,

20   wherein said data structure encryption routine includes causing said cryptographic

21   processor to read said first data structure from said computer readable medium, to

22   execute said internal encryption routine, encrypting said data structure to form said

23   encrypted version of said first data structure, preventing reading information stored

24   in said data records with said computer readable medium removed from said

25   computing system and to write said encrypted version of said first data structure to

26   nonvolatile storage, wherein said first data structure is additionally deleted from said

27   first computer readable medium during execution of said data structure encryption

28   subroutine, and wherein said data structure decryption subroutine includes causing

29   said cryptographic processor to read said encrypted version of said first data

30   structure from nonvolatile storage, to decrypt said encrypted version of said first data

31   structure, forming said first data structure, and to write said first data structure to said

32   computer readable medium, starting at said first location.

1   20. (original): The computing system of claim 19, wherein

2   said first drive unit is a hard drive,

3   said data structure encryption subroutine is executed in response to receiving

4   a request to shut down said computing system, and

5   said data structure decryption subroutine is executed in response to electrical

6   power being turned on within said computing system.

1   21. (original): The computing system of claim 20, wherein

2   said microprocessor is additionally programmed to execute a configuration

3   subroutine providing a user interface for setting and resetting a configuration bit,

4   and

5   said encryption subroutine is executed according to a state of said

6   configuration bit.

1   22. (original): The computing system of claim 21, wherein

2   said encryption subroutine additionally includes setting a flag bit in non-

3   volatile storage, and

4   said decryption subroutine is executed only when said flag bit is set.

1   23. (original): The computing system of claim 19, wherein

2   said computer readable medium is removable,

3   said method additionally comprises a cryptographic selection subroutine

4   providing a graphical user interface,

5   said cryptographic selection subroutine includes displaying a choice between

6   encryption and decryption, displaying representations of computer readable medium

7   in said computing system, and receiving a cryptographic selection signal indicative

8   of whether encryption or decryption is to occur and of a chosen computer readable

9   medium,

10   said encryption subroutine is executed in response to receiving a

11   cryptographic selection signal indicating encryption is to occur, with said first data

12   structure of said chosen computer readable medium being encrypted, and

13   said decryption subroutine is executed in response to receiving a

14   cryptographic selection signal indicating decryption is to occur, and with said

15   encrypted version of said first data structure of said chosen computer readable

16   medium being decrypted.

1   24. (original): The computing system of claim 23, wherein said encrypted version of

2   said first data structure is stored in nonvolatile storage on said chosen computer

3   readable medium.

1   25. (original): The computing system of claim 19, wherein

2   said computer readable medium additionally stores a second data structure,

3   starting at a second location within said computer readable medium, describing

4   characteristics of said first data structure, and

5   said data structure encryption subroutine additionally includes reading said

6   second data structure to determine characteristics of said first data structure.

1   26. (new): A method, within a computing system, providing security for a

2   plurality of data records stored with a first data structure locating data records in

3   said plurality thereof on a computer readable medium within said computing

4   system, wherein said method comprises:

5   encrypting said first data structure to form an encrypted version of said

6   first data structure without encrypting said plurality of data records as said

7   computing system is being shut down, and

8   decrypting said encrypted version of said first data structure as said

9   computing system is being initialized.

1   27. (new): The method of claim 26, wherein said first data record is encrypted

2   with a public key of said computing system and decrypted with a private key of

3   said computing system.

09/919,240   9

1   28. (new): The method of claim 26, additionally comprising:

2   writing said encrypted version of said first data structure to said computer

3   readable medium after encrypting said first data structure; and reading said

4   encrypted version of said first data structure from said computer readable

5   medium before decrypting said encrypted version of said computer readable

6   medium.